AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 3824 Eastview Ave, Las Cruces, New Mexico	Case No. 25-201 MR

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See attachment A, attached hereto and incorporated herein.

located in the New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2261A	Stalking

The application is based on these facts:

See attached Affidavit in Support of an Application for a Search Warrant, attached hereto and incorporated herein.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Lilly Aldana

Applicant's signature

Lilly Aldana, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by submitted electronically and sworn telephonically *(specify reliable electronic means).*

Date: 2/11/25

Judge's signature

City and state: Las Cruces, NM

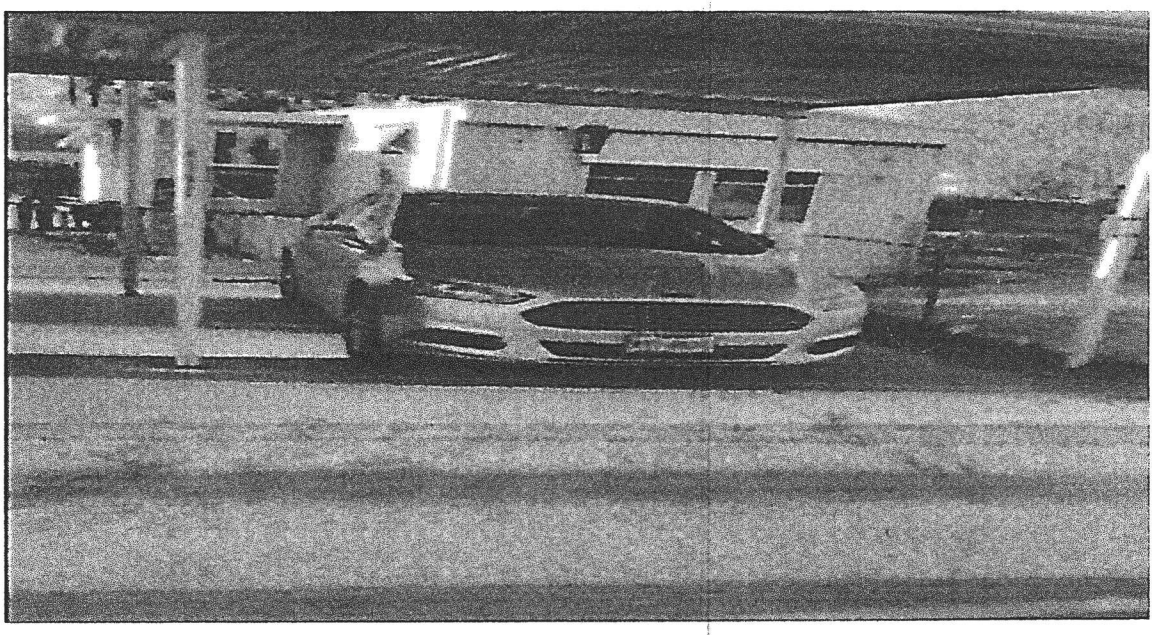
G.J. Fouratt U.S.M.J.

Printed name and title

ATTACHMENT A

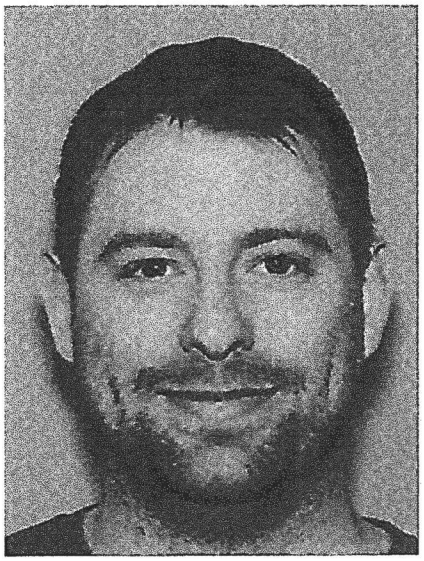
Property to be searched

3824 Eastview Ave, Las Cruces, New Mexico, those areas specific to Robert Earl Talbott or common areas in which items belonging to Robert Earl Talbott might reasonably be found.



ATTACHMENT B

Person to be Arrested at Residence:



Subject: Robert Talbott

Height: 5'10"

Weight: 185lbs

Property to be Seized

1. All records relating to violations of 18 U.S.C. § 2261A(2), those violations involving **Robert Earl Talbott,** and occurring after on or about October of 2024 including:

   a. threatening communications;

   b. any information recording or documenting **Talbott's** schedule or travel from December of 2024 to the present; and

   c. any information concerning **Talbott's** state of mind, motive, or intent.

   d. Firearms

2. All cellular devices, electronic devices, and GPS devices located in the **Subject Premises,** which this warrant further authorizes the forensic examination of any such devices.

That is, FBI New Mexico Division is permitted to transfer any seized evidence and devices to the Dallas Division of the FBI which is located in the Northern District of Texas so forensic examination may be conducted in the district of prosecution of **Talbott**.

3. Computers or storage media used as a means to commit the violations described above.

4. All devices, to include cell phones, tablets, and computers, which may reasonably contain records relating to violations of 18 U.S.C §§ 2261A and 18 U.S.C. § 875 by **Robert Talbott.**

5. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disk drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: 3824 Eastview Ave, Las Cruces, New Mexico	Case No. **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Lilly Aldana, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **3824 Eastview Avenue, Las Cruces, New Mexico 88007;** herein after "**Premises**", further described in Attachment A, for the person and things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 2024. I have gained experience through training and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I earned a Bachelor's degree in Criminal Justice and Master's degree in Criminal Justice. I am classified, trained, and employed as a federal law enforcement officer with statutory arrest authority charged with conducting criminal investigations of alleged violations of federal criminal statutes, including Title 18 of the United States Code. I am currently assigned to the Albuquerque Field Office, Las Cruces Resident Agency, New Mexico. Prior to my current position, I was employed for three years as a Federal Probation Officer with the United States Probation Office, Western District of Texas. I am currently assigned to investigate violations of federal law, including stalking. I am authorized by the Attorney General to request a search warrant.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit is personally known to me based on my training and experience, was gathered or revealed to me personally during the course of this investigation or was gathered or revealed to other sworn law enforcement officers during the course of this investigation and subsequently communicated to me. Based on the information set forth herein, there is probable cause to believe that violations of 18 U.S.C. § 2261A(2) (Stalking) were committed, and that evidence of these violations may be found within the **Premises**.

PROBABLE CAUSE

4. On or about December 23, 2024, the FBI Dallas Field Office received information that **Robert Earl Talbott** (hereinafter "**Talbott**") has been sending threating communications via his cellular telephone number, 214-587-1997, to his wife, A.T. These messages were sent via a facility of interstate commerce to A.T., who resides in Garland, Texas.

5. More specifically, A.T. stated that **Talbott** began threatening her in October 2024 after she obtained a protective order against **Talbott**. However, A.T. later learned the protective order was not served on **Talbott**. A.T. stated **Talbott** sent text messages in October 2024 to his sister to tell A.T. he was going to murder her. **Talbott** also sent A.T. a text message stating "Get your affairs in order cunt this was the last straw. You've got two weeks to live due to travel, make them count."

6. On or about January 14, 2025, the FBI obtained a copy of police reports from the Garland Police Department ("GPD") filed by A.T. concerning **Talbott's** threatening communications. The following is a summary of the reports filed with GPD:

a) In a report dated May 14, 2024, A.T. stated **Talbott** sent A.T. eight text messages telling her to kill herself.

b) In a report dated August 6, 2024, A.T. stated **Talbott** sent her messages to kill herself.

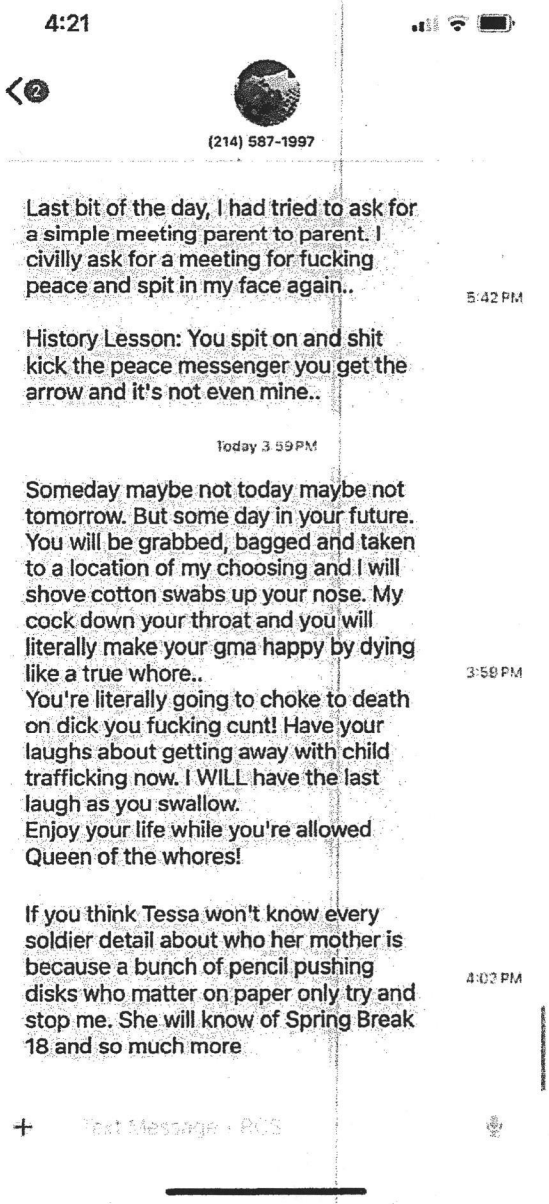
c) In a report dated September 27, 2024, A.T. stated **Talbott** sent her a message stating, "paper doesn't stop a bullet cunt and I know where you live." **Talbott** also sent her a message stating, "in case you think I'm bluffing like last time…sleep with one eye open." **Talbott** sent her the address for both A.T.'s residence and workplace.

d) In a report dated November 5, 2024, A.T. stated **Talbott's** sister sent A.T. a text message from **Talbott** stating, "Tell your bestie [A.T.] im coming to kill her stat."

e) In a report dated December 3, 2024, A.T. stated she received numerous threatening text messages from **Talbott**. One such message in the report stated, "I don't know when but one day, you will be grabbed and a bag put over your head. You will be taken to a location of my choosing, with cotton swabs up your nose and my cock down your throat. You will make your grandma happy by dying like a true whore." A.T. also showed GPD officers a copy of a protective order she had obtained against **Talbott** (DF-23-15828).

f) In a report dated December 17, 2024, A.T. stated that she received a text message from **Talbott**, which she believed to be a violation of the protective order she obtained against **Talbott**. On or about that same date, or shortly thereafter, A.T. learned that the protective order had not been served on **Talbott**. The protective order was subsequently served on **Talbott** on or about December 21, 2024.

7. On or about January 16, 2025, GPD provided a copy of A.T.'s protective order and the text messages to the FBI. The below image was a message saved on or about December 3, 2024, provided by A.T.:



8. On or about January 16, 2025, an open-source check was conducted on Talbott's cellular telephone number. The phone number was registered to **Talbott** at 3824 Eastview Ave Las Cruces, 88007.

9. On January 29, 2025, the FBI interviewed A.T. Through the interview, it was learned that **Talbott** began sending A.T. text messages threatening to kill himself on Superbowl Sunday in 2024, while **Talbott** had their daughter. He also sent A.T. a message threatening to shoot his attorney.

10. A.T. reported that **Talbott** began sending A.T. text messages in May 2024 stating that he was going to get her ex-boyfriend to "get her." **Talbott** also told A.T. her ex-boyfriend should have slit her throat when he had the chance.

11. A.T. said **Talbott** began sending her death threats in October 2024. In December 2024, A.T.'s attorney instructed A.T. and her daughter to flee to the Houston area in response to **Talbott's** messages.

12. A.T. also provided the FBI copies of voicemails from **Talbott**. A summary of the voicemails is below:

a) **Talbott** says he has just crossed state lines and is going to enjoy taking every piece of flesh off of A.T.'s bones and feeding it to her.

b) **Talbott** says A.T. better not be at work or she will miss time to pack and get their daughter out before he kills A.T. in front of their daughter.

c) **Talbott** says A.T. will not be able to come to her phone after he breaks her kneecaps and slits her wrists.

d) **Talbott** says A.T. cannot come to the phone because he has not bashed in her skull yet and he is going to kill her.

e) **Talbott** says he hopes A.T. has enjoyed her job because it will probably be what runs through her mind when he bashes her skull in. **Talbott** says he is either going

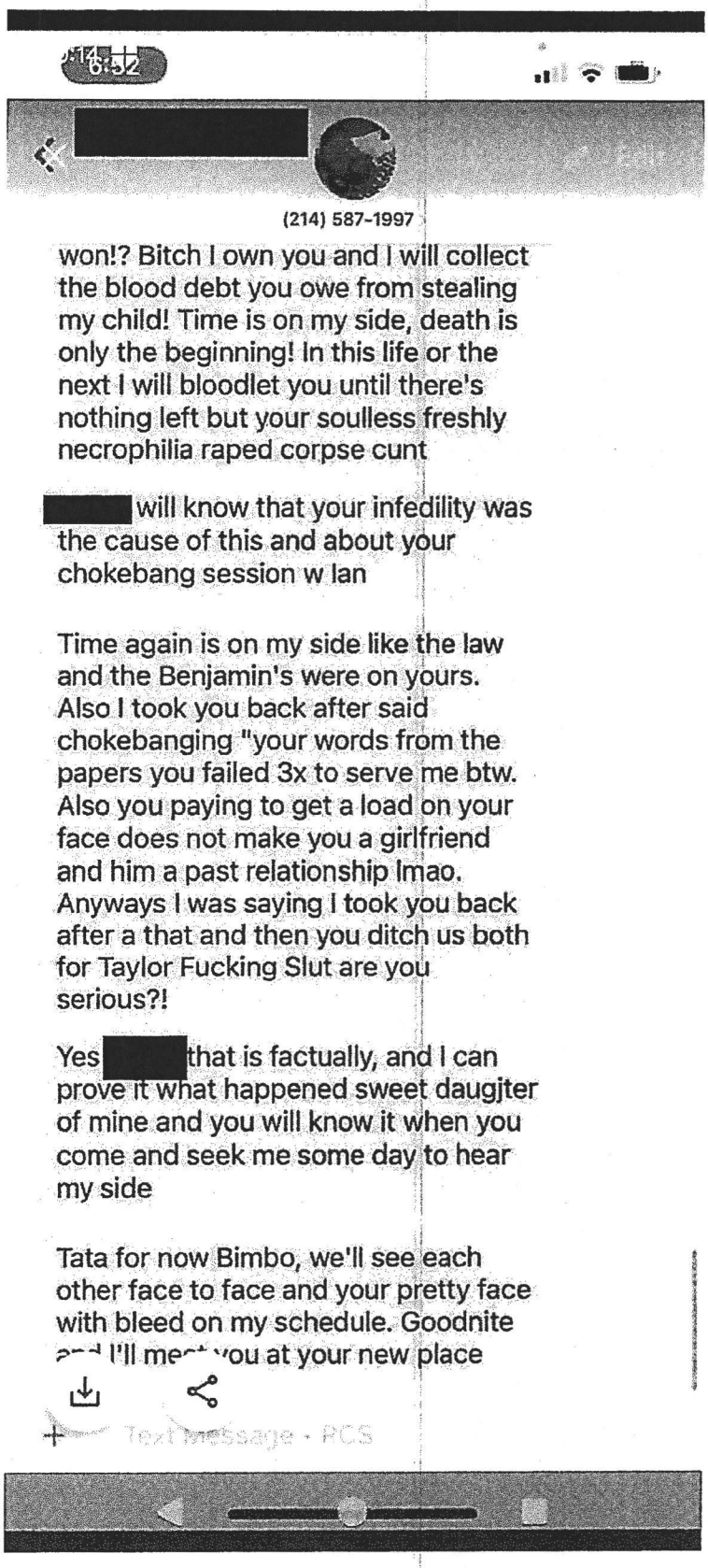
to rape her to death or bash her skull in. **Talbott** says he is coming to Texas right now and A.T. is going to die slowly.

These voicemails were left by **Talbott** using his cellular telephone number 214-587-1997.

13. A.T. has indicated that she knows that **Talbott** has a car and a rifle. Further, **Talbott** has threatened to come to A.T.'s school and church. A.T. is not allowed to take her students out for recess or go on field trips because of the threats.

14. On or about January 30, 2025, A.T. sent the FBI a message stating **Talbott** began sending her text messages again. A.T. provided a screenshot of the message from **Talbott**. The screenshot of the message is below:

[the remainder of this page left intentionally blank]



(214) 587-1997

won!? Bitch I own you and I will collect the blood debt you owe from stealing my child! Time is on my side, death is only the beginning! In this life or the next I will bloodlet you until there's nothing left but your soulless freshly necrophilia raped corpse cunt

[redacted] will know that your infedility was the cause of this and about your chokebang session w Ian

Time again is on my side like the law and the Benjamin's were on yours. Also I took you back after said chokebanging "your words from the papers you failed 3x to serve me btw. Also you paying to get a load on your face does not make you a girlfriend and him a past relationship lmao. Anyways I was saying I took you back after a that and then you ditch us both for Taylor Fucking Slut are you serious?!

Yes [redacted] that is factually, and I can prove it what happened sweet daugjter of mine and you will know it when you come and seek me some day to hear my side

Tata for now Bimbo, we'll see each other face to face and your pretty face with bleed on my schedule. Goodnite and I'll meet you at your new place

Text Message • PCS

15. On or about February 7, 2025, an open source information report revealed that **Talbott** resides at **3824 Eastview Avenue, Las Cruces, New Mexico 88007** (the Subject Premises).

16. A Texas Department of Motor Vehicle report shows that **Talbott** owns a 2016 Ford Fusion sedan, license plate MDT8685 under his name and registered to 3824 Eastview Avenue, Las Cruces, New Mexico 88007. On or about February 7, 2025, through February 10, 2025, multiple spot checks were conducted at the **Subject Premises**. **Talbott's** 2016 Ford Sedan, license plate MDT8685, has been observed parked outside the **Subject Premises** at varying times of day.

17. Additionally, I spoke with Special Agent Sean Macmanus of the FBI Cellular Analysis Survey Team ("CAST"), who has specialized training in cell phone networks and record analysis and has testified as an expert witness to the same. SA Macmanus told me that a preliminary analysis of the T-Mobile call detail records for 214-587-1997 revealed that the activity from the cell phone is consistent with the phone being located at the **Subject Premises**. Additionally, the sector (side) of the cell tower most used by the phone in the set of records was the side of the cell tower in Las Cruces, New Mexico, which provides service to the **Subject Premises**.

18. As described above, **Talbott** has been making threats to the victim via text messages and phone calls, including by leaving voicemail messages. I know from my training and experience that the most common way these messages are sent is using a cellular device (a cellphone). Further, as A.T. resides in Garland, Texas, and **Talbott** resides in Las Cruces, New Mexico, and as these threats were communicated on an electronic device, it is probable that

19. On or about February 3, 2025, **Talbott** was charged by complaint in the Northern District of Texas, for a violation of 18 U.S.C. § 2261A(2). *United States v. Robert Earl Talbott*, No. 3:25-MJ-088-BT (N.D. Tex. Feb. 3, 2025). At that time, an arrest warrant was issued.

20. Although the **Subject Premises** is registered to another individual, the cell phone analysis, open source information and the persistent presence of **Talbott's** vehicle at the **Subject Premises** make it probable that **Talbott** is staying at the **Subject Premises**, and that evidence of the crime, or property used in the crime, would be located at the **Subject Premises**. The FBI therefore requests this warrant to search the **Subject Premises** for **Talbott** and any evidence of, or property involved in, the crime therein.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

22. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **Subject Premises**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). According to 18 U.S. Code § 1030(e)(1) …"the term "computer" means an

electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device…" which includes cell phones.

23. *Probable cause.* I submit that if a computer or storage medium is found in the **Subject Premises**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files and information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes

how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Subject Premises** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to stalk or harass a victim, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make

an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

27. Because other people are believed to share the **Subject Premises** as a residence, it is possible that the **Subject Premises** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

28. Based on the aforementioned information and investigation, I submit that probable cause exists to search the **Subject Premises**, as more particularly described in Attachment A and to seize the items described in Attachment B.

This affidavit was reviewed by AUSA Joni Stahl.

Respectfully submitted,

Lilly Aldana
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on VIA PHONE FEB. 11, 2025.

Honorable
UNITED STATES MAGISTRATE JUDGE